

Response to First Office Action  
Docket No. 002,0200.US.UTLAmendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1        1. (currently amended): A system for providing Web-based remote  
2    security application client administration in a distributed computing environment,  
3    comprising:

4            a self-extracting configuration file containing an executable configuration  
5    file that is self-extractable on a target client into an administered a security  
6    application that is remotely administered by an administrator system;

7            an executable control embedded within an active administration Web  
8    page, the executable control being triggered upon each request for the active Web  
9    page by the administrator system and causing dynamic Web content to be  
10   generated therefrom;

11           a Web server exporting a Web portal comprising the active administration  
12   Web page to a browser application on the administrator system independent of a  
13   specific operating environment and interpreting the executable control to facilitate  
14   copying of the self-extracting configuration file to the target client.

1        2. (original): A system according to Claim 1, further comprising:  
2    the Web server facilitating copying of the self-extracting configuration file  
3    concurrently to a plurality of target clients.

1        3. (original): A system according to Claim 1, further comprising:  
2    the Web server checking administrator credentials while exporting the  
3    Web portal against a list of authorized administrators.

1        4. (original): A system according to Claim 1, further comprising:  
2    the Web server monitoring the status of the copying of the self-extracting  
3    configuration file to at least one target client.

Response to First Office Action  
Docket No. 002.0200.US.UTL

1        5. (original): A system according to Claim 1, further comprising:  
2            the Web server reporting the status of security application configuration  
3            on at least one target client.

1        6. (original): A system according to Claim 1, further comprising:  
2            the self-extracting configuration file performing at least one of an  
3            installation, configuration, updating, and patching of the security application by  
4            executing the executable configuration file.

1        7. (original): A system according to Claim 1, wherein the executable  
2            configuration file comprises at least one of a virus scanning, virus screening,  
3            active security, firewall, and VPN performance reporting application.

1        8. (original): A system according to Claim 1, wherein the executable  
2            configuration file is a cabinet archival file.

1        9. (original): A system according to Claim 1, wherein the active  
2            control is an Active X-compliant control.

1        10. (original): A system according to Claim 1, wherein the distributed  
2            computing environment is TCP/IP-compliant.

1        11. (currently amended): A method for providing Web-based remote  
2            security application client administration in a distributed computing environment,  
3            comprising:  
4            storing a self-extracting configuration file containing an executable  
5            configuration file that is self-extractable on a target client into an administered a  
6            security application that is remotely administered by an administrator system;  
7            providing an executable control embedded within an active administration  
8            Web page, the executable control being triggered upon each request for the active  
9            Web page by the administrator system and causing dynamic Web content to be  
10           generated therefrom;

Response to First Office Action  
Docket No. 002.0200.US.UTL

11           exporting a Web portal comprising the active administration Web page to  
12    a browser application on the administrator system independent of a specific  
13    operating environment; and  
14           interpreting the executable control to facilitate copying of the self-  
15    extracting configuration file to the target client.

1           12. (original): A method according to Claim 11, further comprising:  
2            facilitating copying of the self-extracting configuration file concurrently to  
3    a plurality of target clients.

1           13. (original): A method according to Claim 11, further comprising:  
2            checking administrator credentials while exporting the Web portal against  
3    a list of authorized administrators.

1           14. (original): A method according to Claim 11, further comprising:  
2            monitoring the status of the copying of the self-extracting configuration  
3    file to at least one target client.

1           15. (original): A method according to Claim 11, further comprising:  
2            reporting the status of security application configuration on at least one  
3    target client.

1           16. (original): A method according to Claim 11, further comprising:  
2            performing at least one of an installation, configuration, updating, and  
3    patching of the security application by executing the executable configuration file.

1           17. (original): A method according to Claim 11, wherein the  
2    executable configuration file comprises at least one of a virus scanning, virus  
3    screening, active security, firewall, and VPN performance reporting application.

1           18. (original): A method according to Claim 11, wherein the  
2    executable configuration file is a cabinet archival file.

Response to First Office Action  
Docket No. 002.0200.US.UTL

1        19. (original): A method according to Claim 11, wherein the active  
2 control is an Active X-compliant control.

1        20. (original): A method according to Claim 11, wherein the  
2 distributed computing environment is TCP/IP-compliant.

1        21. (original): A computer-readable storage medium holding code for  
2 performing the method according to Claim 11.

1        22. (currently amended): A system for remotely administering a client  
2 application using a Web-based portal in a TCP/IP-compliant environment,  
3 comprising:

4            an archival configuration file capable of self-extracting on a target client  
5 into an executable configuration file;  
6            an executable control embedded into an active administration Web page,  
7 the executable control being triggered upon each request for the active Web page  
8 by a requesting administrator and causing dynamic Web content to be generated  
9 therefrom;

10           a Web server serving the active administration Web page to a browser  
11 application to [[a]] the requesting administrator, comprising:  
12            a security module confirming credentials for the requesting  
13 administrator against a list of authorized administrators; and  
14            a transfer module interpreting the executable control upon  
15 successful credentialing to facilitate substantially concurrent copying of the self-  
16 extracting configuration file to at least one target client.

1        23. (original): A system according to Claim 22, further comprising:  
2            the Web server continuously monitoring the status of the copying of the  
3 self-extracting configuration file to the at least one target client; and  
4            the Web server generating a status event upon completion of the copying.

1        24. (original): A system according to Claim 22, further comprising:

Response to First Office Action  
Docket No. 002.0200.US.UTL

2 the Web server reporting the status of each application configuration on  
3 the at least one target client.

1 25. (original): A system according to Claim 22, wherein the active  
2 control is an Active X-compliant control.

1 26. (currently amended): A method for remotely administering a client  
2 application using a Web-based portal in a TCP/IP-compliant environment,  
3 comprising:

4 storing an archival configuration file capable of self-extracting on a target  
5 client into an executable configuration file;

6 embedding an executable control into an active administration Web page,  
7 the executable control being triggered upon each request for the active Web page  
8 by a requesting administrator and causing dynamic Web content to be generated  
9 therefrom;

10 serving the active administration Web page to a browser application to  
11 [[a]] the requesting administrator, comprising:

12 confirming credentials for the requesting administrator against a  
13 list of authorized administrators; and

14 interpreting the executable control upon successful credentialing to  
15 facilitate substantially concurrent copying of the self-extracting configuration file  
16 to at least one target client.

1 27. (original): A method according to Claim 26, further comprising:  
2 continuously monitoring the status of the copying of the self-extracting  
3 configuration file to the at least one target client; and  
4 generating a status event upon completion of the copying.

1 28. (original): A method according to Claim 26, further comprising:  
2 reporting the status of each application configuration on the at least one  
3 target client.

Response to First Office Action  
Docket No. 002.0200.US.UTL

1        29. (original): A method according to Claim 26, wherein the active  
2        control is an Active X-compliant control.

1        30. (original): A computer-readable storage medium holding code for  
2        performing the method according to Claim 26.